

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): Young-Hyun KIM
SERIAL NO.: Not yet assigned
FILED: Herewith
FOR: **MOBILE TERMINAL FOR USE RESTRICTION AND
COPYRIGHT PROTECTION FOR CONTENT, AND
CONTENT SECURITY SYSTEM USING THE SAME**
DATED: February 9, 2004

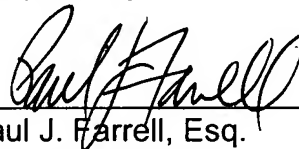
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY DOCUMENTS

Sir:

Enclosed is a certified copy of Korean Patent Appln. No.
2003-8251 filed on February 10, 2003, from which priority is claimed under 35
U.S.C. §119.

Respectfully submitted,



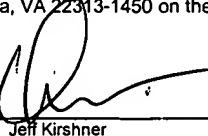
Paul J. Farrell, Esq.
Reg. No. 33,494
Attorney for Applicant(s)

DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, NY 11553
(516) 228-8484

CERTIFICATION UNDER 37 C.F.R. 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service in an envelope as "Express Mail Post Office to Addressee" Mail Label Number EL 995744831 US addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date listed below.

Dated: February 9, 2004


Jeff Kirshner



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원 번호 : 10-2003-0008251
Application Number

출원 년 월 일 : 2003년 02월 10일
Date of Application
FEB 10, 2003

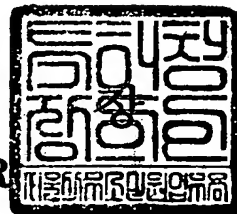
출원인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 03 월 27 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0005
【제출일자】	2003.02.10
【국제특허분류】	H04B
【발명의 명칭】	컨텐츠에 대한 사용 제한 및 저작권 보호를 위한 통신 단말기 및 컨텐츠 보안 시스템
【발명의 영문명칭】	COMMUNICATION TERMINAL FOR PROTECTING COPYRIGHT AND RESTRICTING USING OF CONTENTS AND CONTENTS SECURITY SYSTEM USING THAT
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	2003-001449-1
【발명자】	
【성명의 국문표기】	김영현
【성명의 영문표기】	KIM, Young Hyun
【주민등록번호】	750227-2231747
【우편번호】	152-093
【주소】	서울특별시 구로구 개봉3동 289-5
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 이건주 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	8 면 8,000 원

1020030008251

출력 일자: 2003/4/1

【우선권주장료】	0	건	0	원
【심사청구료】	12	항	493,000	원
【합계】	530,000			원

【요약서】**【요약】**

컨텐츠에 대한 사용 제한 및 저작권 보호를 위한 통신 단말기가 개시된다. 통신 단말기는, 설정된 제품정보와 고유번호 및 컨텐츠를 저장하고 외부 기기로부터 제공된 컨텐츠의 암호화를 위한 암호키를 저장하는 저장부, 외부 기기와 상호 데이터의 송수신을 위한 인터페이스를 제공하는 통신부, 암호키를 이용하여 고유번호 및 컨텐츠를 암호화하는 암호부, 통신부를 통해 암호화된 컨텐츠를 외부 기기에 업로드하고 입력되는 명령에 따라 업로드된 컨텐츠의 다운로드 요구신호를 외부 기기에 전송하는 제어부, 및 컨텐츠의 다운로드 요구신호에 대응하여 외부 기기로부터 다운로드된 컨텐츠를 암호키를 이용하여 복호하는 복호부를 갖는다. 컨텐츠를 외부 저장장치에 업로드한 통신단말기만 추후에 업로드된 컨텐츠를 다운로드할 수 있음에 따라 컨텐츠에 대한 보안을 유지할 수 있다.

【대표도】

도 2

【색인어】

통신단말기, 휴대폰, 컨텐츠, 유료, 보안, 다운로드, 업로드, 암호

【명세서】**【발명의 명칭】**

컨텐츠에 대한 사용 제한 및 저작권 보호를 위한 통신 단말기 및 컨텐츠 보안 시스템
{COMMUNICATION TERMINAL FOR PROTECTING COPYRIGHT AND RESTRICTING USING OF CONTENTS
AND CONTENTS SECURITY SYSTEM USING THAT}

【도면의 간단한 설명】

도 1은 통신단말기를 이용한 유료컨텐츠 다운로드 및 업로드 시스템의 일반적인 구성을 도시한 블록도,

도 2는 본 발명에 따른 컨텐츠에 대한 저작권을 보호하기 위한 컨텐츠 보안 시스템의 바람직한 실시예를 도시한 블록도,

도 3은 본 발명에 따른 컨텐츠 보안 시스템을 이용한 컨텐츠 보호방법의 바람직한 실시예를 도시한 순서도, 그리고

도 4는 도 3에 의해 업로드된 컨텐츠를 다운로드하는 과정을 나타낸 순서도이다.

* 도면의 주요 부분에 대한 부호의 설명 *

100 : 통신단말기 110 : 무선통신부

120 : 음성처리부 130 : 제어부

140 : 키입력부 150 : 표시부

160 : 저장부 170, 260 : 암호부

180, 270 : 복호부 190 : 유선통신부

200 : 컴퓨터 210 : CPU

240 : 인터페이스 280 : 보조기억장치

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 콘텐츠를 다운로드 및 업로드하는 통신단말기에 관한 것으로서, 보다 상세하게는, 콘텐츠에 대한 보안성을 유지하면서 콘텐츠를 다운로드 및 업로드할 수 있는 통신 단말기에 관한 것이다.

<14> 최근 들어, 무선 단말기는 상대방과 음성 및 화상을 통해 상호 통화하는데 이용되는 것 외에도, 게임, 음악 감상, 노래방 기능, 및 캐릭터 이미지 등과 같은 다양한 콘텐츠를 다운로드 받고 이것을 이용하여 다양한 기능을 사용자에게 제공할 수 있다. 기존에 무선 단말기에서 데이터 통신을 이용하여 콘텐츠를 다운로드하는 기능은, 컴퓨터에 저장된 콘텐츠를 무선 단말기로 전송하는 단 방향(one way)방식만이 가능하다. 일반적으로 무선 단말기의 사용자들은 콘텐츠서버를 운영하는 제공자에게 소정의 비용을 지불하고, 콘텐츠서버에 접속하여 해당 콘텐츠를 다운로드한다. 이러한 비용 부담으로 인해 사용자가 개인적으로 콘텐츠를 작성하여 이용하고자 하는 경우, 데이터 통신으로 콘텐츠를 다운로드하여 이용하는 것을 유용하나 질적인 면에서 콘텐츠 유료서비스에 비해 떨어지고 있다.

- <15> 콘텐츠 유료서비스를 이용하여 다운 받은 콘텐츠들을 더 이상 저장할 공간이 무선 단말기에 남아있지 않은 경우, 사용자들은 자신들이 비용을 지불하고 유료로 다운 받은 콘텐츠들을 삭제한 후 새로운 콘텐츠들을 콘텐츠 유료서비스를 이용하여 무선단말기로 다운로드할 수밖에 없다.
- <16> 기존에 제공되는 유료 콘텐츠 서비스는 콘텐츠서버로부터 유료콘텐츠를 다운로드하는 기능만을 제공할 뿐, 유료콘텐츠를 다운로드하고 필요에 따라 다운로드된 유료콘텐츠를 콘텐츠서버에 업로드하는 기능을 제공하지 않고 있다.
- <17> 또한, 기존의 무선단말기는 PC링크 등과 같은 인터페이스를 통해 컴퓨터와 연결되어 사용자들이 편집한 콘텐츠들을 다운로드하는 기능만을 제공한다. 이때, 무선단말기에서 사용자의 컴퓨터로 저장된 콘텐츠를 전송하는 기능이 가능한 경우, 컴퓨터에 저장된 콘텐츠들을 모든 다른 무선단말기에도 다운로드하는 것이 가능하게 되므로 유료콘텐츠에 대한 저작권을 보호받을 수 없는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

- <18> 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 무선단말기에서 유료서비스로 다운로드 받은 유료콘텐츠들을 컴퓨터와 연계하여 다운로드 및 업로드할 때 유료콘텐츠들에 대한 사용 권한을 제한할 수 있는 통신단말기 및 이를 이용한 콘텐츠 보안 시스템을 제공하는데 있다.
- <19> 본 발명의 다른 목적은, 무선단말기에 다운로드된 유료콘텐츠들이 저장된 컴퓨터에 접속된 임의의 무선단말기에 상기 유료콘텐츠들을 임의로 제공하는 것을 예방하여 유료

컨텐츠들에 대한 저작권을 보호할 수 있는 통신단말기 및 이를 이용한 컨텐츠 보안 시스템을 제공하는데 있다.

【발명의 구성 및 작용】

<20> 상기와 같은 목적은 본 발명에 따라, 유선 및/또는 무선으로 컨텐츠서버에 접속하여 컨텐츠를 제공받아 외부 기기에 상기 컨텐츠를 업로드하는 통신단말기에 있어서, 설정된 제품정보와 고유번호 및 컨텐츠를 저장하고, 외부 기기로부터 제공된 컨텐츠의 암호화를 위한 암호키를 저장하는 저장부; 외부 기기와 상호 데이터의 송수신을 위한 인터페이스를 제공하는 통신부; 암호키를 이용하여 고유번호 및 컨텐츠를 암호화하는 암호부; 통신부를 통해 암호화된 컨텐츠를 외부 기기에 업로드하고, 입력되는 명령에 따라 업로드된 컨텐츠의 다운로드 요구신호를 외부 기기에 전송하는 제어부; 및 컨텐츠의 다운로드 요구신호에 대응하여 외부 기기로부터 다운로드된 컨텐츠를 암호키를 이용하여 복호하는 복호부를 포함하는 통신 단말기에 의해 달성된다.

<21> 바람직하게는, 상기 암호키는 통신단말기의 제품정보와 고유번호, 및 외부 기기에 설정된 시간정보를 고려하여 생성한다.

<22> 상기와 같은 목적은 본 발명에 따라, 컨텐츠서버로부터 제공된 컨텐츠를 외부 디바이스로부터 제공된 암호키를 이용하여 암호화하여 상기 외부 디바이스에 업로드하는 통신단말기; 및 상기 통신단말기의 모델정보와 고유번호 중 적어도 어느 하나를 고려하여 상기 암호키를 생성하고, 통신단말기로부터 업로드된 암호화된 컨텐츠를 저장하는 외부 저장장치를 포함하는 컨텐츠 보안 시스템에 의해 달성된다.

- <23> 바람직하게는, 상기 외부 저장장치는 암호키를 생성할 때, 외부 저장장치에 설정된 시간정보를 더 고려하여 암호키를 생성한다. 또한, 상기 외부 저장장치는 외부 저장장치에 설정된 시간정보와 통신단말기에 설정된 시간정보의 일치 여부를 비교하여, 각각의 시간정보가 일치하는 경우 암호키를 생성한다.
- <24> 상기 통신단말기는 입력되는 명령에 따라 기 업로드된 콘텐츠의 다운로드 요구신호를 외부 저장장치에 전송하고, 콘텐츠의 다운로드 요구신호에 대응하여 외부 저장장치로부터 다운로드된 콘텐츠를 암호키를 이용하여 복호화한다.
- <25> 한편, 상기와 같은 목적은 본 발명에 따라, 콘텐츠서버로부터 콘텐츠를 제공받는 통신단말기 및 통신단말기의 요구에 따라 콘텐츠를 저장하는 외부 저장장치를 구비한 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법에 있어서, 입력되는 명령에 따라 콘텐츠 업로드 요구신호를 상기 외부 저장장치에 전송하는 단계; 콘텐츠 업로드 요구신호에 대응하여 외부 저장장치로부터 요구된 통신단말기의 모델정보 및 고유번호를 상기 외부 저장장치에 전송하는 단계; 모델정보 및 고유번호가 고려되어 상기 외부 저장장치에서 생성된 암호키를 이용하여 업로드하기 위한 콘텐츠를 암호화하는 단계; 및 암호키에 의해 암호화된 콘텐츠를 외부 저장장치에 전송하는 단계를 포함하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법에 의해 달성된다.
- <26> 바람직하게는, 본 발명의 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법은, 통신단말기에서 업로드된 암호화된 콘텐츠가 암호키에 의해 암호화된 것인지를 판단하는 단계; 및 암호화된 콘텐츠가 암호키에 의해 암호화된 것으로 판단되면, 암호화된 콘텐츠를 저장하는 단계를 더 포함한다. 또한, 본 발명의 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법은, 기 업로드된 콘텐츠의 다운로드 명령이 입력되면, 콘텐츠 다운로드 요구신호

를 외부 저장장치에 전송하는 단계; 콘텐츠 다운로드 요구신호에 대응하여 외부 저장장치로부터 제공된 콘텐츠 인덱스정보 중 다운로드를 위한 콘텐츠 인덱스정보가 선택되면, 선택된 콘텐츠 인덱스정보를 외부 저장장치에 전송하는 단계; 및 선택된 콘텐츠 인덱스정보에 대응하여 외부 저장장치로부터 암호화된 콘텐츠가 다운로드되면, 다운로드된 암호화된 콘텐츠를 암호키를 이용하여 복호하는 단계를 더 포함한다.

- <27> 상기 암호키는 외부 저장장치에 설정된 시간정보가 더 고려되어 외부 저장장치에 의해 생성되는 것이 바람직하다. 또한, 상기 암호키는 외부 저장장치에 의해, 외부 저장장치에 설정된 시간정보와 통신단말기에 설정된 시간정보의 일치 여부가 비교되어 각각의 시간정보가 일치하는 경우 생성된다.
- <28> 본 발명에 따르면, 콘텐츠를 외부 저장장치에 업로드할 때 대상 콘텐츠를 외부 저장장치로부터 제공된 암호키를 이용하여 암호화하고 암호화된 콘텐츠를 외부 저장장치에 업로드함으로써, 콘텐츠를 외부 저장장치에 업로드한 통신단말기만 추후에 업로드된 콘텐츠를 다운로드할 수 있음에 따라 콘텐츠에 대한 보안을 유지할 수 있다.
- <29> 또한, 업로드한 콘텐츠의 다운로드 요구에 대응하여 저장된 콘텐츠를 제공받아 업로드시 암호화에 이용된 암호키(k)를 이용하여 복호함으로써, 콘텐츠의 업로드 시 이용된 암호키(k)에 의해서만 다운로드된 콘텐츠를 복호함에 따라 콘텐츠에 대한 사용 권한을 제한할 수 있다.
- <30> 그리고, 통신단말기의 모델정보(M) 및 고유번호(N)를 포함하는 콘텐츠 다운로드를 요구함에 따라 다운로드를 요구한 콘텐츠가 통신단말기에 의해 기 업로드된 콘텐츠인지를 판별하여 선택적으로 콘텐츠를 통신단말기에 제공함으로써, 콘텐츠에 대한 저작권을 보호할 수 있다.

- <31> 이하, 본 발명의 바람직한 실시예들을 첨부한 도면을 참조하여 상세히 설명한다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.
- <32> 도 1은 통신단말기를 이용한 유료컨텐츠 다운로드 및 업로드 시스템의 일반적인 구성을 도시한 블록도이다.
- <33> 통신단말기(12)는 입력되는 신호에 따라 유료컨텐츠를 제공하는 컨텐츠서버(22)에 접속하고, 선택된 신호에 따라 이동통신망(14)을 통해 컨텐츠서버(22)에 유료컨텐츠의 제공을 요구하는 신호를 전송한다. 무선통신서버(16)는 이동통신망(14)을 통해 전송된 유료컨텐츠 요구신호를 유선통신서버(18)에 전송한다. 이때 무선통신서버(16)는 이동통신망(14)에 접속되어 무선으로 통신을 수행하는 단말기의 통신 채널을 제어하고, 요구되는 명령에 대응하는 신호를 해당 단말기에 제공한다. 유선통신서버(18)는 유선통신망(20)에 접속되어 유선으로 통신을 수행하는 단말기의 통신 채널을 제어하고, 요구되는 명령에 대응하는 신호를 해당 단말기에 제공한다.
- <34> 유선통신서버(18)는 통신단말기(12)의 유료컨텐츠 요구신호가 수신되면, 수신된 유료컨텐츠 요구신호를 유선통신망(20)을 통해 컨텐츠서버(22)에 전송한다. 컨텐츠서버(22)는 유료컨텐츠 요구신호가 수신되면, 수신된 요구신호에 대응하는 컨텐츠를 통신단말기(12)에 전송하도록 유선통신망(20)을 통해 유선통신서버(18)에 전송한다. 유선통신서버(18)는 컨텐츠서버(22)로부터 전송된 컨텐츠가 수신되면, 수신된 컨텐츠를 무선통신서버(16)에 전송한다. 무선통신서버(16)는 유선통신서버(18)로부터 전송된 컨텐츠를 이동통신망(14)을 통해 통신단말기(12)에 전송한다.

- <35> 이에 따라, 통신단말기(12)는 유료컨텐츠 요구신호에 대응하는 컨텐츠를 수신받게 된다. 통신단말기(12)는 수신된 컨텐츠를 설정 및/또는 입력되는 명령에 따라 화면에 표시하거나 메모리에 저장할 수 있다. 또한, 통신단말기(12)는 외부 컴퓨터(10)와 인터넷을 통해 연결되어, 저장된 컨텐츠를 컴퓨터(10)에 업로드할 수 있다. 이에 따라, 컴퓨터(10)는 통신단말기(12)로부터 출력된 컨텐츠를 마련된 보조기억장치에 저장한다.
- <36> 이러한 컨텐츠 다운로드 및 업로드를 위한 일반적인 통신시스템은 통신단말기(12)에 저장된 컨텐츠를 컴퓨터(10)와 같은 외부 저장장치에 업로드하여 통신단말기(12)의 한정된 저장 공간의 약점을 해소할 수 있으나, 컴퓨터(10)에 저장된 컨텐츠에 대한 보안성이 떨어질 수 있다.
- <37> 도 2는 본 발명에 따른 컨텐츠에 대한 저작권을 보호하기 위한 컨텐츠 보안 시스템의 바람직한 실시예를 도시한 블록도이다. 도시된 바와 같이, 컨텐츠 보안 시스템은 통신단말기(100) 및 외부 저장장치의 예로서 컴퓨터(200)를 갖는다.
- <38> 통신단말기(100)는 안테나(50)를 통해 컨텐츠서버(22)에 컨텐츠를 요구하고, 수신된 컨텐츠를 저장부(160)에 저장하며, 저장부(160)에 저장된 컨텐츠를 유선통신부(190)를 통해 연결된 컴퓨터(200)에 업로드한다. 이때, 유선통신부(190)는 통신단말기(10)와 컴퓨터(200) 간에 근거리 내에서 무선으로 통신이 가능한 기능을 제공하는 근거리 무선 통신부로 대체할 수도 있다.
- <39> 도시된 통신단말기(100)는 제어부(130), 무선통신부(110), 음성처리부(120), 키입력부(140), 표시부(150), 저장부(160), 및 유선통신부(190)를 갖는다.

- <40> 제어부(130)는 통신단말기(100)의 전반적인 동작을 제어하고, 외부 디바이스와 상호 통신을 위한 신호의 송수신을 제어한다. 무선통신부(110)는 통신 가능한 외부 디바이스와 상호 통신을 수행하고, 외부 디바이스로부터 전송된 콘텐츠를 비롯한 데이터를 수신한다. 음성처리부(120)는 무선통신부(110)로부터 출력된 신호를 디코딩하여 전기적인 음성 신호로 변환한 후 스피커(122)로 출력한다. 또한 음성처리부(120)는 마이크(124)에 독취된 음향신호를 전기적인 신호로 변환하여 코딩한 후 송신부(118)로 출력한다.
- <41> 키입력부(140)는 다수의 숫자키 및 문자키를 구비하며, 선택된 키에 대응하는 데이터를 발생하여 제어부(130)로 전송한다. 표시부(150)는 제어부(130)의 제어에 따라 통신단말기(100)의 상태정보 및/또는 동작정보를 화면에 표시한다. 저장부(160)에는 제어부(130)의 제어 시 필요한 구동 프로그램 및 제어 동작 시 발생하는 데이터를 임시 저장된다. 또한 저장부(160)에는 다운로드한 콘텐츠가 저장된다. 유선통신부(190)는 컴퓨터(200) 등과 같은 외부 통신장치와 유선으로 상호 통신을 수행하기 위한 인터페이스를 제공한다.
- <42> 한편, 도면의 무선통신부(110)는, 듀플렉서(112), 수신부(114), 주파수합성부(116), 송신부(118)를 갖는다.
- <43> 듀플렉서(112)는 안테나(50)에 수신되는 신호 중 설정된 주파수대역 신호를 추출하여 수신부(114)로 출력한다. 또한, 듀플렉서(112)는 송신부(118)로부터 출력되는 신호를 안테나(50)로 출력한다. 수신부(114)는 제어부(130)의 제어에 의해 수신된 신호 중 음성신호에 해당하는 데이터는 음성처리부(120)로 출력하며, 음성신호가 아닌 데이터는 제어부(130)로 출력한다.

- <44> 주파수합성부(116)는 제어부(130)의 제어에 의해 송신부(118)와 수신부(114)로 출력할 주파수를 발생하여 각각 출력한다. 송신부(118)는 음성처리부(120)로부터 출력되는 신호와 주파수합성부(116)로부터 출력되는 신호를 송신을 위해 설정된 주파수대역의 신호로 변환한다.
- <45> 한편, 본 실시예에 따라 콘텐츠 보안 시스템의 통신단말기(100)에는 암호부(170) 및 복호부(180)가 마련된다. 암호부(170)는 컴퓨터(200)로부터 제공된 암호키(k)를 이용하여 통신단말기(100)의 고유번호(N) 및 저장부(160)에 저장된 콘텐츠 등을 암호화한다. 이때 암호화된 고유번호(N(k)) 및 콘텐츠(C(k))는 제어부(130)의 제어에 따라 유선통신부(190)를 통해 컴퓨터(200)에 전송, 즉 업로드된다. 복호부(180)는 컴퓨터(200)에 업로드된 콘텐츠(C(k))가 유선통신부(190)를 통해 수신되면, 제어부(130)의 제어에 따라 수신된 콘텐츠(C(k))를 복호화한다.
- <46> 따라서, 콘텐츠를 외부 저장장치에 업로드할 때 대상 콘텐츠를 외부 저장장치로부터 제공된 암호키를 이용하여 암호화하고 암호화된 콘텐츠를 외부 저장장치에 업로드함으로써, 콘텐츠를 외부 저장장치에 업로드한 통신단말기만 추후에 업로드된 콘텐츠를 다운로드할 수 있음에 따라 콘텐츠에 대한 보안을 유지할 수 있다. 이에 따라, 콘텐츠서버로부터 콘텐츠를 제공한 제공자의 콘텐츠에 대한 저작권을 보호할 수 있다.
- <47> 한편, 도면의 컴퓨터(200)는 CPU(Central Processing Unit)(210), RAM(Random Access Memory)(220), ROM(Read-Only Memory)(230), 인터페이스(240), 입출력부(250), 암호부(260), 복호부(270), 및 보조기억장치(280)를 갖는다.

- <48> CPU(210)는 컴퓨터(200) 프로그램의 명령어를 처리하기 위한 논리회로를 마련하고 있으며, 컴퓨터(200)의 전반적인 동작을 제어하고, 입력되는 신호에 따라 해당 데이터를 처리한다. RAM(220)은 컴퓨터(200) 프로세서가 빠르게 접근할 수 있도록 하기 위하여, 운영체제, 응용프로그램 및 현재 사용중인 데이터를 유지하고 있는 저장 장소이다. ROM(230)은 컴퓨터(200)에 미리 장착되어 있는 메모리로서, 저장되어 있는 데이터는 읽을 수만 있고 그 값을 변경할 수는 없는 것이 일반적이다. ROM(230)은 컴퓨터(200)를 켤 때마다 부팅되거나 재 설정하기 위한 프로그램을 저장하고 있다.
- <49> 인터페이스(240)는 외부 디바이스와 상호 데이터 교환을 위한 프로토콜을 제공한다. 본 실시예에서 인터페이스(240)는 통신단말기(100)의 유선통신부(190)와 연결되어 통신단말기(100)와 컴퓨터(200) 간에 상호 데이터 교환을 위한 프로토콜을 제공한다. 입출력부(250)는 컴퓨터(200)에 연결된 키보드 및 마우스 등과 같은 입력장치로부터 입력된 신호를 CPU(210)에 제공하고, CPU(210)의 제어에 따라 해당 데이터를 컴퓨터(200)에 연결된 모니터 등과 같은 출력장치로 출력한다.
- <50> 암호부(260)는 통신단말기(100)로부터 제공된 통신단말기(100)의 모델정보(M), 고유번호(N), 및 컴퓨터(200)에 설정된 시간정보(T)를 기초로, 통신단말기(100)에 제공하기 위한 암호키(k)를 생성한다. 복호부(270)는 통신단말기(100)로부터 제공된 암호화된 콘텐츠(C(k))를 복호화하여, 통신단말기(100)로부터 제공된 콘텐츠(C(k))가 컴퓨터(200)에서 제공한 암호키(k)에 의해 암호화된 콘텐츠인지를 체크한다.
- <51> 보조기억장치(280)에는 통신단말기(100)의 모델정보(M), 고유번호(N), 및 컴퓨터(200)에 설정된 시간정보(T)를 기초로 암호부(260)에서 생성한 암호키(k)(282) 및 컴퓨터(100)로부터 제공된 콘텐츠(C(k))(284)가 저장된다.

- <52> 통신단말기(100)가 업로드한 콘텐츠의 다운로드를 컴퓨터(200)에 요구하는 경우, 컴퓨터(200)는 보조기억장치(280)에 저장된 콘텐츠(284)를 통신단말기(100)에 제공한다. 이때 통신단말기(100)에 제공되는 콘텐츠는 암호키(k)로 암호화된 데이터이다. 이에 따라, 통신단말기(100)는 암호화된 콘텐츠가 수신되면, 컴퓨터(200)로부터 기 제공되어 저장부(160)에 저장된 암호키(k)를 이용하여 암호화된 콘텐츠를 복호한다.
- <53> 바람직하게는, 통신단말기(100)는 컴퓨터(200)에 콘텐츠의 다운로드를 요구할 때, 통신단말기(100)의 모델정보(M) 및 고유번호(N)를 포함하여 컴퓨터(200)에 콘텐츠 다운로드를 요구할 수 있다. 이에 따라, 컴퓨터(200)의 CPU(210)는 콘텐츠 다운로드 요구신호에 포함된 통신단말기(100)의 모델정보(M) 및 고유번호(N)를 통해, 다운로드를 요구하는 콘텐츠가 기존에 통신단말기(100)에서 업로드한 콘텐츠인지를 판별한다. 다운로드를 요구한 콘텐츠가 통신단말기(100)에서 업로드한 콘텐츠인 것으로 판단되면, CPU(210)는 보조기억장치(280)에 저장된 암호화된 콘텐츠(284)를 인터페이스(240)를 통해 통신단말기(100)에 전송한다. 이때, 다운로드를 요구한 콘텐츠가 통신단말기(100)에서 업로드한 콘텐츠가 아닌 것으로 판단되면, CPU(210)는 보조기억장치(280)에 저장된 암호화된 콘텐츠(284)를 통신단말기(100)에 제공하지 않는다.
- <54> 따라서, 업로드한 콘텐츠의 다운로드 요구에 대응하여 저장된 콘텐츠를 제공받아 업로드시 암호화에 이용된 암호키(k)를 이용하여 복호함으로써, 콘텐츠의 업로드 시 이용된 암호키(k)에 의해서만 다운로드된 콘텐츠를 복호함에 따라 콘텐츠에 대한 사용 권한을 제한할 수 있다. 또한, 통신단말기(100)의 모델정보(M) 및 고유번호(N)를 포함하는 콘텐츠 다운로드를 요구함에 따라 다운로드를 요구한 콘텐츠가 통신단말기(100)에 의

해 기 업로드된 콘텐츠인지를 판별하여 선택적으로 콘텐츠를 통신단말기(100)에 제공함으로써, 콘텐츠에 대한 저작권을 보호할 수 있다.

<55> 도 3은 본 발명에 따른 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법의 바람직한 실시예를 도시한 순서도이다.

<56> 먼저, 통신단말기(100)의 제어부(130)는 키입력부(140)에 마련된 소정의 키를 이용하여 저장부(160)에 저장된 콘텐츠를 업로드하기 위한 신호가 입력되면, 입력된 콘텐츠 업로드 요구신호를 유선통신부(190)를 통해 컴퓨터(200)에 전송한다(S100). 컴퓨터(200)의 CPU(210)는 통신단말기(100)로부터 전송된 콘텐츠 업로드 요구신호가 수신되면, 통신단말기(100)의 모델정보(M) 및 고유번호(N)의 전송을 요청하는 신호를 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S105).

<57> 통신단말기(100)의 제어부(130)는 모델정보(M) 및 고유번호(N)의 전송을 요청하는 신호가 수신되면, 저장부(160)에 저장된 통신단말기(100)의 모델정보(M) 및 고유번호(N)를 유선통신부(190)를 통해 컴퓨터(200)에 전송한다(S110). 통신단말기(100)의 모델정보(M) 및 고유번호(N)가 수신되면, 컴퓨터(200)의 CPU(210)는 통신단말기(100)의 모델정보(M)와 고유번호(N), 및 컴퓨터(200)에 설정된 시간정보(T)를 이용하여 통신단말기(100)에서 콘텐츠를 암호화하는데 이용될 암호키(k)를 생성하도록 암호부(260)를 제어한다. 이에 따라, 암호부(260)는 통신단말기(100)의 모델정보(M)와 고유번호(N), 및 컴퓨터(200)에 설정된 시간정보(T)를 기초로 암호키(k)를 생성한다(S120). 이때, CPU(210)는 암호부(260)에서 생성된 암호키(k)를 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S130).

<58> 한편, 컴퓨터(200)의 암호부(260)에서 시간정보(T)를 고려하여 암호키(k)를 생성할 때, 암호부(260)는 컴퓨터(200)에 설정된 시간정보(T)와 통신단말기(100)에 설정된 시간정보를 고려하는 것이 바람직하다. 암호부(260)는 컴퓨터(200)에 설정된 시간정보(T)와 통신단말기(100)에 설정된 시간정보가 다른 경우, 암호키(k)를 생성하지 않는 것이 바람직하다.

<59> 통신단말기(100)의 제어부(130)는 컴퓨터(200)로부터 전송된 암호키(k)가 수신되면, 암호키(k)를 이용하여 통신단말기(100)의 고유번호(N)를 암호화하도록 암호부(170)를 제어한다. 이에 따라, 암호부(170)는 암호키(k)를 이용하여 통신단말기(100)의 고유번호(N)를 암호화한다(S140). 이때, 제어부(130)는 암호부(170)에서 암호화된 통신단말기(100)의 고유번호(N(k))를 유선통신부(190)를 통해 컴퓨터(200)에 전송한다(S150).

<60> 통신단말기(100)에서 전송한 암호화된 통신단말기(100)의 고유번호(N(k))가 수신되면, CPU(210)는 수신된 고유번호(N(k))를 복호하도록 복호부(270)를 제어한다(S160). 이에 따라, 복호부(270)는 암호키(k)를 이용하여 고유번호(N(k))를 복호화한다. 이때, CPU(210)는 복호된 고유번호를 통해 통신단말기(100)에서 암호키(k)를 이용하여 고유번호(N)를 암호화하는 동작이 정상적으로 수행되는지를 판단한다. 통신단말기(100)에서 암호키(k)를 이용하여 고유번호(N)를 정상적으로 암호화하는 것으로 판단되면, CPU(210)는 콘텐츠 전송을 허락하는 명령을 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S170).

<61> 통신단말기(100)의 제어부(130)는 콘텐츠 전송 허락 명령이 수신되면, 저장부(160)에 저장된 콘텐츠에 대한 콘텐츠 인덱스 정보를 전송한다(S180). 콘텐츠 인덱스 정보로

는 콘텐츠의 종류, 명칭, 및 파일 형식 등을 예로 들 수 있다. 컴퓨터(200)의 CPU(210)는 수신된 콘텐츠 인덱스 정보를 입출력부(250)를 통해 화면에 표시하도록 하고, 표시된 콘텐츠 인덱스 정보 중 어느 하나가 선택되면 선택된 콘텐츠 인덱스 정보를 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S190).

<62> 통신단말기(100)의 제어부(130)는 콘텐츠 인덱스 정보가 수신되면, 저장부(160)로부터 수신된 콘텐츠 인덱스 정보에 대응하는 콘텐츠를 인출하고 인출된 콘텐츠를 암호화하도록 암호부(170)를 제어한다(S200). 이에 따라, 암호부(170)는 암호키(k)를 이용하여 제어부(130)에서 제공된 콘텐츠를 암호화한다. 이때 제어부(130)는 암호화된 콘텐츠(C(k))를 유선통신부(190)를 통해 컴퓨터(200)에 전송한다.

<63> 컴퓨터(200)의 CPU(210)는 인터페이스(240)를 통해 수신되는 콘텐츠(C(k))가 암호부(260)에 의해 생성된 암호키(k)를 이용하여 암호된 것인지를 판단하기 위해, 수신된 콘텐츠(C(k))를 복호화하도록 복호부(270)를 제어한다(S210). 이에 따라, 복호부(270)에서 복호된 콘텐츠가 암호키(k)에 의해 암호화된 것으로 판단되면, CPU(210)는 암호키(k)에 의해 암호화된 콘텐츠(C(k))를 보조기억장치(280)에 저장한다(S220).

<64> 따라서, 통신단말기(100)에 저장된 콘텐츠를 컴퓨터(200)에서 통신단말기(100)의 모델정보(M), 고유번호(N), 및 컴퓨터(200)에 설정된 시간정보(T)를 기초로 생성된 암호키(k)를 이용하여 암호화하여 컴퓨터(200)에 업로드함으로써, 임의의 통신단말기가 컴퓨터(200)에 저장된 콘텐츠(C(k))를 다운로드하여 복호할 수 없기 때문에 콘텐츠의 사용을 제한할 수 있다.

<65> 도 4는 도 3에 의해 업로드된 콘텐츠를 다운로드하는 과정을 나타낸 순서도이다.

- <66> 먼저, 통신단말기(100)의 제어부(130)는 키입력부(140)로부터 업로드된 콘텐츠의 다운로드를 요구하는 신호가 입력되면, 콘텐츠 다운로드 요구신호를 유선통신부(190)를 통해 컴퓨터(200)로 전송한다(S300). 컴퓨터(200)의 CPU(210)는 보조기억장치(280)에 저장된 콘텐츠의 인덱스 정보를 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S310).
- <67> 통신단말기(100)의 제어부(130)는 수신된 콘텐츠 인덱스 정보로부터 적어도 어느 하나에 대한 다운로드 선택신호가 입력되면, 입력된 다운로드 받기 위한 콘텐츠의 인덱스정보를 유선통신부(190)를 통해 컴퓨터(200)에 전송한다(S320). 컴퓨터(200)의 CPU(210)는 수신된 다운로드 받기 위한 콘텐츠의 인덱스정보에 대응하는 콘텐츠를 보조기억장치(280)로부터 인출하여 인터페이스(240)를 통해 통신단말기(100)에 전송한다(S330).
- <68> 통신단말기(100)의 제어부(130)는 컴퓨터(200)로부터 전송된 콘텐츠가 수신되면, 수신된 콘텐츠를 복호하도록 복호부(180)를 제어한다(S340). 이에 따라, 복호부(180)는 저장부(160)에 저장된 암호키(k)를 이용하여 수신된 콘텐츠를 복호화한다. 이때, 제어부(130)는 복호화된 콘텐츠를 저장부(160)에 저장한다(S350).
- <69> 따라서, 콘텐츠의 업로드시에 콘텐츠를 암호화할 때 이용한 암호키(k)를 통해서만 다운로드된 콘텐츠를 복호하도록 함으로써, 콘텐츠의 무분별한 제공을 막을 수 있고 이에 따라 콘텐츠의 저작권을 보호할 수 있다.

【발명의 효과】

- <70> 본 발명에 따르면, 콘텐츠를 외부 저장장치에 업로드할 때 대상 콘텐츠를 외부 저장장치로부터 제공된 암호키를 이용하여 암호화하고 암호화된 콘텐츠를 외부 저장장치에 업로드함으로써, 콘텐츠를 외부 저장장치에 업로드한 통신단말기만 추후에 업로드된 콘텐츠를 다운로드할 수 있음에 따라 콘텐츠에 대한 보안을 유지할 수 있다.
- <71> 또한, 업로드한 콘텐츠의 다운로드 요구에 대응하여 저장된 콘텐츠를 제공받아 업로드시 암호화에 이용된 암호키(k)를 이용하여 복호함으로써, 콘텐츠의 업로드시 이용된 암호키(k)에 의해서만 다운로드된 콘텐츠를 복호함에 따라 콘텐츠에 대한 사용 권한을 제한할 수 있다.
- <72> 그리고, 통신단말기의 모델정보(M) 및 고유번호(N)를 포함하는 콘텐츠 다운로드를 요구함에 따라 다운로드를 요구한 콘텐츠가 통신단말기에 의해 기 업로드된 콘텐츠인지를 판별하여 선택적으로 콘텐츠를 통신단말기에 제공함으로써, 콘텐츠에 대한 저작권을 보호할 수 있다.
- <73> 이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능할 것이다.

【특허청구범위】**【청구항 1】**

유선 및/또는 무선으로 컨텐츠서버에 접속하여 컨텐츠를 제공받아 외부 기기에 상기 컨텐츠를 업로드하는 통신단말기에 있어서,

설정된 제품정보와 고유번호 및 상기 컨텐츠를 저장하고, 상기 외부 기기로부터 제공된 상기 컨텐츠의 암호화를 위한 암호키를 저장하는 저장부;

상기 외부 기기와 상호 데이터의 송수신을 위한 인터페이스를 제공하는 통신부;

상기 암호키를 이용하여 상기 고유번호 및 상기 컨텐츠를 암호화하는 암호부;

상기 통신부를 통해 상기 암호화된 컨텐츠를 상기 외부 기기에 업로드하고, 입력되는 명령에 따라 상기 업로드된 컨텐츠의 다운로드 요구신호를 상기 외부 기기에 전송하는 제어부; 및

상기 컨텐츠의 다운로드 요구신호에 대응하여 상기 외부 기기로부터 다운로드된 컨텐츠를 상기 암호키를 이용하여 복호하는 복호부를 포함하는 것을 특징으로 하는 통신 단말기.

【청구항 2】

제 1항에 있어서,

상기 암호키는 상기 제품정보 및 상기 고유번호 중 적어도 하나를 기초로 상기 외부 기기에 의해 생성되는 것을 특징으로 하는 통신 단말기.

【청구항 3】

제 2항에 있어서,

상기 암호키는 상기 외부 기기에 설정된 시간정보를 더 고려하여 상기 외부 기기에 의해 생성되는 것을 특징으로 하는 통신 단말기.

【청구항 4】

컨텐츠서버로부터 제공된 컨텐츠를 외부 디바이스로부터 제공된 암호키를 이용하여 암호화하여 상기 외부 디바이스에 업로드하는 통신단말기; 및

상기 통신단말기의 모델정보와 고유번호 중 적어도 어느 하나를 고려하여 상기 암호키를 생성하고, 상기 통신단말기로부터 업로드된 암호화된 컨텐츠를 저장하는 외부 저장장치를 포함하는 것을 특징으로 하는 컨텐츠 보안 시스템.

【청구항 5】

제 4항에 있어서,

상기 외부 저장장치는 상기 암호키를 생성할 때, 상기 외부 저장장치에 설정된 시간정보를 더 고려하여 상기 암호키를 생성하는 것을 특징으로 하는 컨텐츠 보안 시스템.

【청구항 6】

제 5항에 있어서,

상기 외부 저장장치는 상기 외부 저장장치에 설정된 시간정보와 상기 통신단말기에 설정된 시간정보의 일치 여부를 비교하여, 각각의 상기 시간정보가 일치하는 경우 상기 암호키를 생성하는 것을 특징으로 하는 콘텐츠 보안 시스템.

【청구항 7】

제 6항에 있어서,

상기 통신단말기는 입력되는 명령에 따라 기 업로드된 콘텐츠의 다운로드 요구신호를 상기 외부 저장장치에 전송하고, 상기 콘텐츠의 다운로드 요구신호에 대응하여 상기 외부 저장장치로부터 다운로드된 콘텐츠를 상기 암호키를 이용하여 복호화하는 것을 특징으로 하는 콘텐츠 보안 시스템.

【청구항 8】

콘텐츠서버로부터 콘텐츠를 제공받는 통신단말기 및 상기 통신단말기의 요구에 따라 상기 콘텐츠를 저장하는 외부 저장장치를 구비한 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법에 있어서,

입력되는 명령에 따라 콘텐츠 업로드 요구신호를 상기 외부 저장장치에 전송하는 단계;

상기 콘텐츠 업로드 요구신호에 대응하여 상기 외부 저장장치로부터 요구된 상기 통신단말기의 모델정보 및 고유번호를 상기 외부 저장장치에 전송하는 단계;

상기 모델정보 및 상기 고유번호가 고려되어 상기 외부 저장장치에서 생성된 암호키를 이용하여 업로드하기 위한 콘텐츠를 암호화하는 단계; 및

상기 암호키에 의해 암호화된 콘텐츠를 상기 외부 저장장치에 전송하는 단계를 포함하는 것을 특징으로 하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법.

【청구항 9】

제 8항에 있어서,

상기 통신단말기에서 업로드된 상기 암호화된 콘텐츠가 상기 암호키에 의해 암호화된 것인지를 판단하는 단계; 및

상기 암호화된 콘텐츠가 상기 암호키에 의해 암호화된 것으로 판단되면, 상기 암호화된 콘텐츠를 저장하는 단계를 더 포함하는 것을 특징으로 하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법.

【청구항 10】

제 9항에 있어서,

기 업로드된 상기 콘텐츠의 다운로드 명령이 입력되면, 콘텐츠 다운로드 요구신호를 상기 외부 저장장치에 전송하는 단계;

상기 콘텐츠 다운로드 요구신호에 대응하여 상기 외부 저장장치로부터 제공된 콘텐츠 인덱스정보 중 다운로드를 위한 콘텐츠 인덱스정보가 선택되면, 선택된 콘텐츠 인덱스정보를 상기 외부 저장장치에 전송하는 단계; 및

상기 선택된 콘텐츠 인덱스정보에 대응하여 상기 외부 저장장치로부터 암호화된 콘텐츠가 다운로드되면, 상기 다운로드된 암호화된 콘텐츠를 상기 암호키를 이용하여 복호하는 단계를 더 포함하는 것을 특징으로 하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법.

【청구항 11】

제 10항에 있어서,

상기 암호키는 상기 외부 저장장치에 설정된 시간정보를 더 고려하여 상기 외부 저장장치에 의해 생성되는 것을 특징으로 하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법.

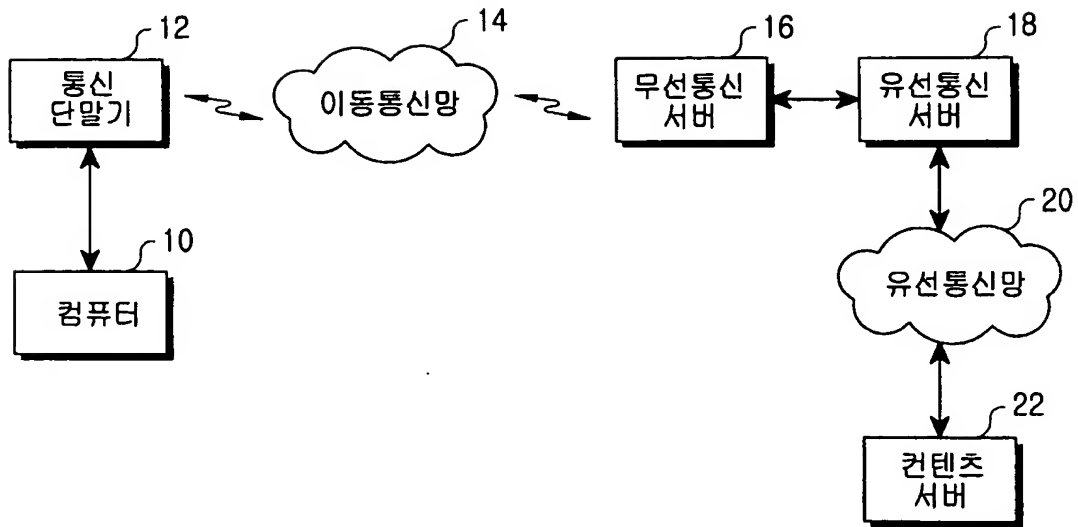
【청구항 12】

제 11항에 있어서,

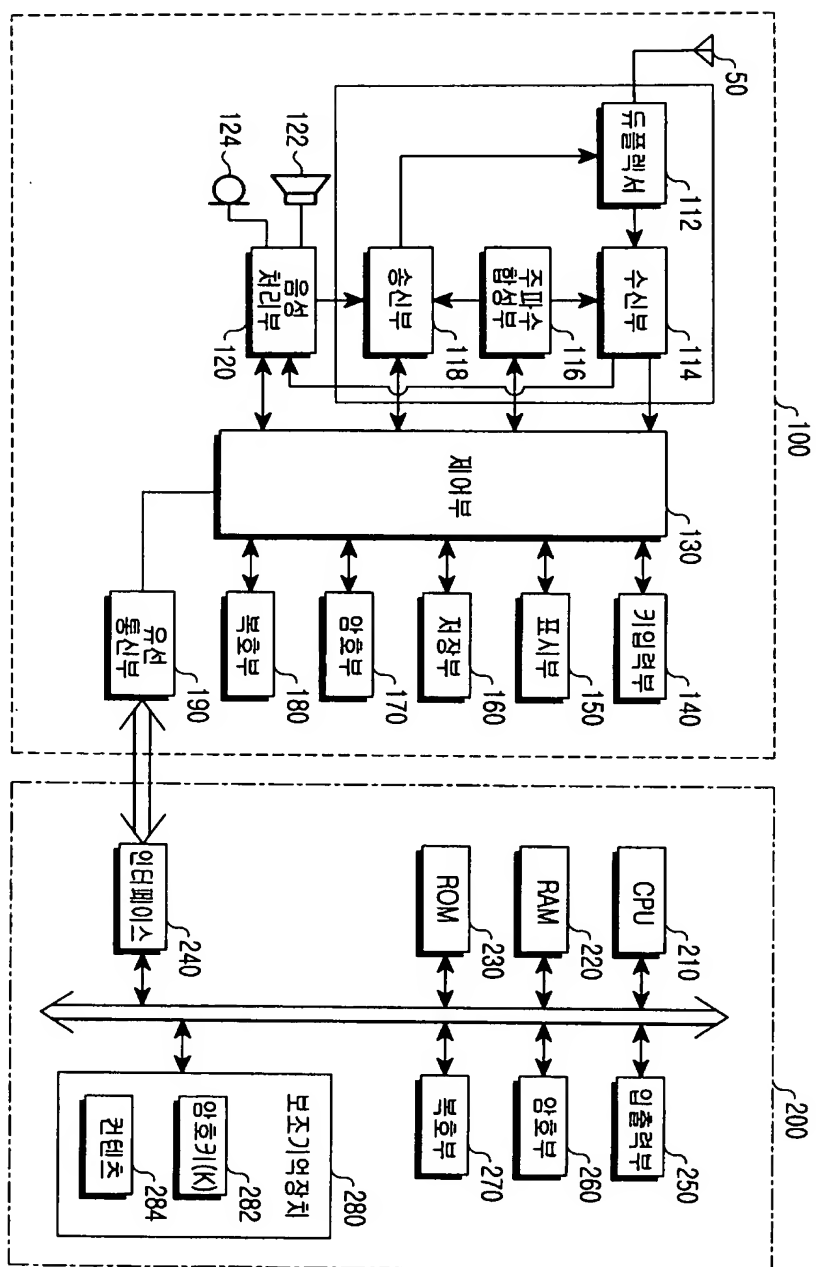
상기 암호키는 상기 외부 저장장치에 의해, 상기 외부 저장장치에 설정된 시간정보와 상기 통신단말기에 설정된 시간정보의 일치 여부가 비교되어 각각의 상기 시간정보가 일치하는 경우 생성되는 것을 특징으로 하는 콘텐츠 보안 시스템을 이용한 콘텐츠 보호방법.

【도면】

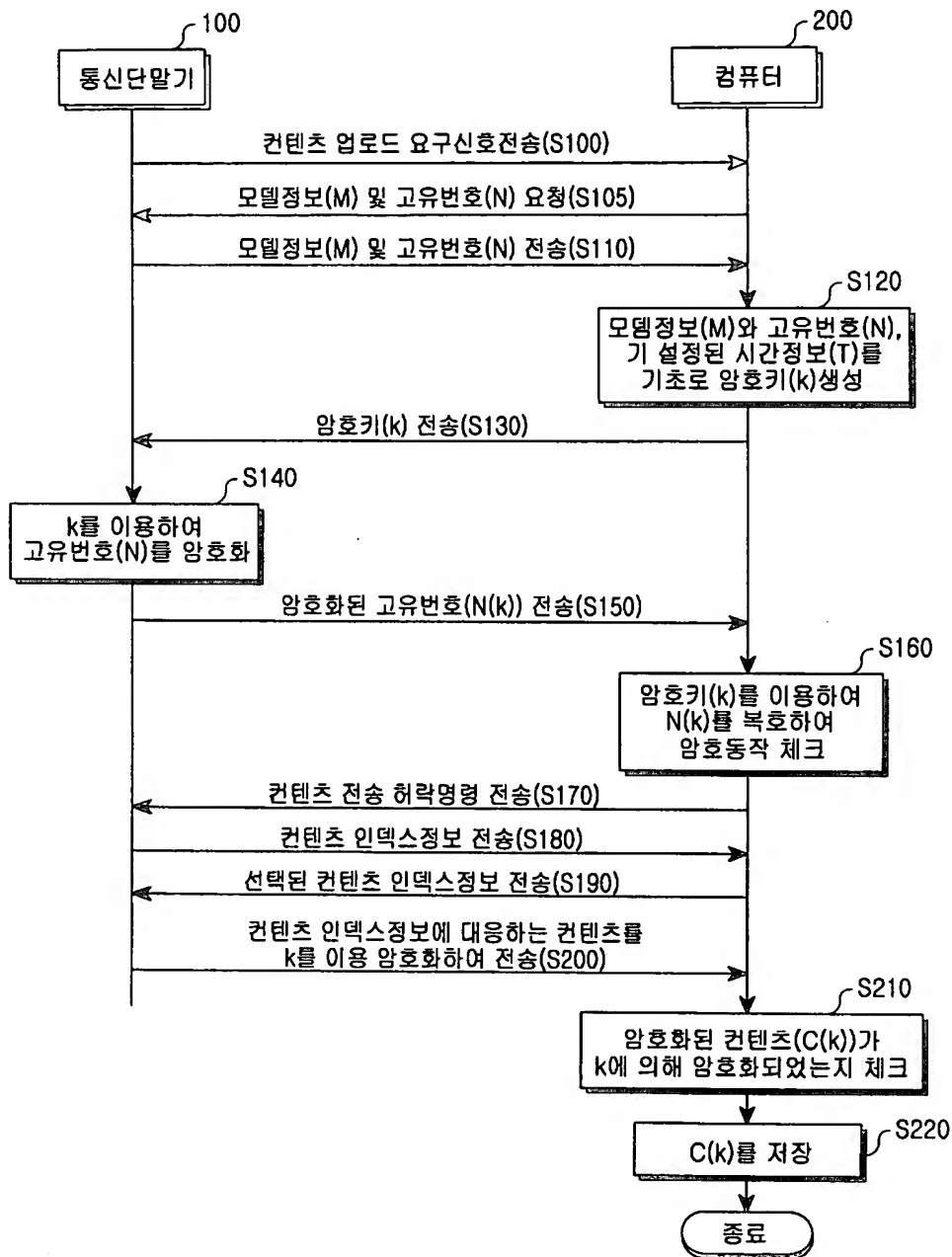
【도 1】



【도 2】



【도 3】



【도 4】

